Government's Evolving Role in Digital Transformation

Highlights from a private government roundtable, hosted by the Advanced Technology Academic Research Center (ATARC), in partnership with Indr, July 2023

The federal government's role in driving digital transformation is ever evolving as technology rapidly accelerates. A heightened risk of cyber attacks and the rising expectations of constituents are pushing the government's transformation efforts, while also making the roles and responsibilities of government IT more intricate and unpredictable.

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Indr, federal IT experts discussed the complex challenges and opportunities surrounding digital transformation in government.

The Evolution of Digital Transformation

Panelists shared snapshots of their digital transformation journeys, starting with migrating legacy systems to the cloud. All agencies represented at the roundtable have largely completed cloud migration and are now optimizing these cloud-based systems to their agency's unique mission requirements.

As technology advances at an increasingly rapid pace, agencies are also working to understand and manage the risks associated with modernization. This is especially true for artificial intelligence. Some agencies are working on operationalizing AI risk management frameworks to ensure an aligned use of AI.

The emergence of AI has quickly brought to light numerous ethical challenges with its use in government, particularly with data validation. Agencies must not only ensure internal actors use information ethically, but also find ways to mitigate internal threats when they occur.

"Everything is all about AI right now, and it's crazy. I've never seen anything in my career that has changed the environment so much as generative AI has in the last six months."

The Challenges with Cloud Migration

Some agencies did not have a choice whether or not to migrate to the cloud. Computing capacity quickly outgrew servers that were confined to basement storage, and as a result agencies made plans to migrate servers to the cloud. Some agencies on the panel initiated a "lift and shift" approach to cloud migration, which was conducted in stages in an order that made sense to the mission.

Agencies have been largely successful with cloud migration endeavors, partly due to the vigorous testing conducted before putting the new cloud servers into production. Good planning ensured end users could not detect a difference in environments. As one participant noted, "If you do [cloud migration] right, no one really knows."

One panelist shared their modernization success in which processing was improved by as much as 4 times, with the same personnel and resources. They achieved this by analyzing workflows, identifying bottlenecks, and determining where technology could improve processes.

However, agencies must find ways to manage the risk of operating cloud systems while leveraging new technology advantages like artificial intelligence. Agencies will need to spend considerable time ensuring safeguards are in place for AI use. However, it's still unclear how agencies will continuously validate these controls once in place.

One panelist shared their success with resiliency testing. Every few months agencies will test major systems by taking them down and investigating the failures. This exercise identifies vulnerabilities within and between systems. As AI advances, agencies will need to adopt a similar testing regime.

The Challenge of New Priorities

With new technology comes new Executive Orders (EOs). While agencies follow the guidance of EOs, each agency is responsible for creating policies to align their operations with the EO. One panelist notes this practice will become challenging as agencies across government develop different policies surrounding AI use. They argue that all agencies must be on the same page when it comes to developing AI policy.

Agencies are also focused on Zero Trust and identity management—an area that's particularly challenging when external partners need access to government systems. Identity access management is a complex issue unique to every agency and mission, which makes it virtually impossible to deploy a one-size-fits-all solution. As a security model, one panelist suggests Zero Trust applies to many of the complex challenges associated with artificial intelligence.

One panelist questioned the potential use of AI to redact sensitive documents, a notoriously time-consuming and tedious task. While simple on the surface, achieving this may be more complex as security is taken into account. The AI that drives the redaction could become vulnerable, not just the data itself. This is just one of many scenarios that panelists expect to confront in the future as AI is introduced in government.

The Workforce Challenge

Chief among challenges facing the government is finding and hiring skilled AI and cybersecurity experts who are duty-bound to serve. Panelists shared their struggles competing with the private sector for skilled talent. Marketing campaigns, high-value skills training, and maintaining a friendly and helpful work environment are some of the ways panelists are recruiting and retaining talent.

"You don't hear when things go right, you definitely hear when things go wrong."

Measuring digital transformation is tricky. This is especially true when measuring the success of cyber security initiatives, since success lies in what did not occur. On the other hand, if a cyber attack did occur and the agency paid for systems intended to prevent the attack, the costly incident makes it harder to justify digital investments.

Measuring success and process of digital transformation efforts will differ for the type of business, such as in gigabytes of data or service uptime. Other panelists measure results by adversarial actions against their systems and make adjustments based on these events. Ultimately, one panelist notes, its staff who can determine how well something is working and where the problems and opportunities are located.

Final Thoughts

- AI will bring many benefits to the government, especially with intelligence. It will help agencies find early warnings and indications faster, and search through disperate data to find weak spots and vulnerabilities. However, the problem is deploying AI. There must be safeguards in place before AI is deployed.

- EO is a guiding foundation, but agencies must also align on policy. Addressing AI as one government is critically important.

- Agencies must understand the risks associated with AI systems. AI use cases are different from what agencies are traditionally used to, and agencies must begin to think about AI use cases differently. Agencies should also consider which stakeholders are best able to articulate the risks associated with AI.

- When thinking about integrating AI, agencies should take a holistic view of their technology ecosystem to determine where new technology fits. Using a multi-year strategy, agencies can continue to move forward without losing sight of the big picture.

- Find and leverage experts within the organization who will be using the technology and work backwards from a human design perspective. While AI technology is around the corner, agencies should not lose sight of the role humans play in digital transformation.